****

Havenbedrijf Amsterdam

MOBI

Methodiek vOor EEN ObjectiEve BEVEILIGINGSINVENTARISATIE

AANVRAAG FORMULIER

ISPS CERTIFICERING

**INHOUDSOPGAVE**

[**H1. Bedrijfsinformatie** 3](#_Toc443467697)

[**1.1 Havenfaciliteit gegevens** 3](#_Toc443467698)

[**1.2 Beschrijving van de havenfaciliteit** 3](#_Toc443467699)

[**1.3 Gegevens van de Port Facility Security Officer (PFSO)** 4](#_Toc443467700)

[**1.4 Gegevens van de plaatsvervangend PFSO** 4](#_Toc443467701)

[**H2. Toetsingsteam** 5](#_Toc443467702)

[**2.1 Gegevens 1e toetser** 5](#_Toc443467703)

[**2.2 Gegevens 2e toetser** 5](#_Toc443467704)

[**H3. Toelichting Aanvraagformulier** 6](#_Toc443467705)

[**H4. Begrippenlijst** 7](#_Toc443467706)

[**H5 Questionnaire bij aanvraag tot certificering van een havenfaciliteit** 9](#_Toc443467707)

[**H6. Deel 2: veiligheidsbewustzijn (security awareness)** 13](#_Toc443467708)

[**H7. Ondertekening** 20](#_Toc443467709)

[**Bijlagen** 21](#_Toc443467710)

[**Risicolanden** 21](#_Toc443467711)



MOBI is door Havenbedrijf Amsterdam gelicenseerd onder de licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 4.0 Internationaal. Ga naar <http://creativecommons.org/licenses/by-nc-sa/4.0/> om een kopie van de licentie te kunnen lezen.

# **H1. Bedrijfsinformatie**

**1.1 Havenfaciliteit gegevens**

|  |
| --- |
| Bedrijfsnaam : Type hier uw bedrijfsnaam.Postadres : Type hier het postadres van uw bedrijf.Postcode : Type hier de postcode.Plaats : Type hier de plaatsnaam.Havenfaciliteitnaam : Type hier de volledige naam van uw havenfaciliteit (terminal).Adres : Type hier het adres van de terminal.Postcode : Type hier de postcode.Plaats : Type hier de plaatsnaam.Oeverfront nummer : Type hier het haven of oeverfront nummer.Valt onder BRZO : Geef hier aan of uw bedrijf onder de BRZO valt.Aantal zeeschepen : Geef hier aan hoeveel zeeschepen u ontvangt op jaarbasis.Permanent ISPS : Geef hier aan of uw terminal permanent ISPS beveiligd is.Versienummer PFSP : Type hier het versienummer van uw beveiligingsplan. |

**1.2 Beschrijving van de havenfaciliteit**Waaronder: Bedrijfsprocessen, ladingbehandeling, bedrijfskenmerken etc.

*(Beschrijf hier uw terminal. Indien u dit al in een bestaand beveiligingsplan heeft beschreven, kunt u deze herzien en hier overnemen)*

##  **1.3 Gegevens van de Port Facility Security Officer (PFSO)**

|  |
| --- |
| Naam : Type hier de volledige naam van de PFSO.Functie : Type de volledige functie.Email : Type het e-mail adres.Telefoonnummer : Type het telefoonnummer.Mobiel : Type het mobiele telefoonnummer.  |

## **1.4 Gegevens van de plaatsvervangend PFSO**

|  |
| --- |
| Naam : Type hier de volledige naam van de plaatsvervangend PFSO.Functie : Type de volledige functie.Email : Type het e-mail adres.Telefoonnummer : Type het telefoonnummer.Mobiel : Type het mobiele telefoonnummer.  |

# **H2. Toetsingsteam**

(Bij controle van het aanvraagformulier, in te vullen door toetsingsteam)

## **2.1 Gegevens 1e toetser**

|  |
| --- |
| Naam : Type hier de volledige naam van de 1e toetser.Functie : Type de volledige functie.Telefoonnummer : Type het telefoonnummer.E-mail : Type het e-mail adres.Datum : Type hier de datum.Handtekening : |

## **2.2 Gegevens 2e toetser**

|  |
| --- |
| Naam : Type de volledige naam van de 2e toetser.Functie : Type de volledige functie.Telefoonnummer : Type het telefoonnummer.E-mail : Type het e-mail adres.Datum : Type hier de datum.Handtekening : |

# **H3. Toelichting Aanvraagformulier**

U wilt ISPS-plichtige zeeschepen[[1]](#footnote-1) op uw havenfaciliteit ontvangen. Conform de havenbeveiligingswet dient uw faciliteit hiertoe gecertificeerd te worden. Dit houdt in dat er een veiligheidsbeoordeling (risico analyse) plaatsvindt en dat u op basis van deze beoordeling beveiligingsmaatregelen neemt, die u in een beveiligingsplan beschrijft. Het Port Security Toetsingsteam voert, namens de bevoegde autoriteit, de veiligheidsbeoordeling uit en toetst of de door beschreven en geïmplementeerde maatregelen aan de ISPS-code voldoen. Een uitgebreide beschrijving van dit proces vind u in het document *Procesbeschrijving ISPS Certificering*.

Met behulp van dit aanvraagformulier initieert u het certificeringsproces. Door het formulier aan het toetsingsteam te sturen, doet een verzoek tot de veiligheidsbeoordeling.

Om de veiligheidsbeoordeling uit te kunnen voeren dient het Port Security Toetsingsteam over diverse gegevens te beschikken; deze worden in dit formulier aan u gevraagd. De uiteindelijke veiligheidsbeoordeling ontvangt u als besluit van de bevoegde autoriteit en bestaat onder meer uit een risico inventarisatie en een actielijst welke aangeeft wat uw faciliteit nog dient te implementeren om gecertificeerd te worden. Dit kunnen zowel fysieke maatregelen (hekwerken e.d.) als procedurele maatregelen zijn.

In het aanvraag formulier wordt onderscheid gemaakt tussen een feitelijk blok (vragen 1 t/m 7) en een subjectief blok (vragen 8 t/m 12). De antwoorden in het feitelijke blok, hebben invloed op de risico inventarisatie. De gegevens uit het subjectieve blok geven de veiligheidsbeleving/cultuur van uw organisatie weer.

De gegevens die in het feitelijk blok gevraagd worden hebben een relatie met:

* Het type faciliteit;
* Gevaarlijke stoffen;
* Locatie in de haven en buurtbedrijven;
* Verwachte hoeveelheid te ontvangen schepen;
* Verwachte verblijfsduur van de schepen;
* Vlaggenstaat van de verwachte schepen;
* Herkomst / bestemming van de lading.

De gegevens in het subjectieve blok betreffen:

* Het veiligheidsbewustzijn;
* De historie van de havenfaciliteit m.b.t. incidenten;
* De digitale beïnvloedbaarheid van de systemen (cybersecurity).

Ten aanzien van het invullen van de vragenlijst is het belangrijk om te realiseren dat de focus op de maritieme beveiliging ligt; en niet zo zeer op veiligheidsaspecten als operationele veiligheid of persoonlijke veiligheid. Externe veiligheid is daar en tegen wel onderdeel van de vragenlijst.

# **H4. Begrippenlijst**

|  |  |
| --- | --- |
| Begrip | Definitie/duiding |
| Risicocontour 10-⁶ | Indicatie van een afstand die geldt tussen risicobronnen en kwetsbare objecten. Een risicocontour (ofwel plaatsgebonden risico) geeft aan hoe groot in de omgeving de overlijdenskans is door een ongeval met een risicobron: binnen de contour is het risico groter, buiten de contour is het risico kleiner. Bij een plaatsgebonden risico van 10-6 is de kans dat er daadwerkelijk een zwaar ongeval plaatsvindt 1 op de miljoen. Risicocontouren worden op een risicokaart weergegeven. Deze toont contouren bij inrichtingen, installaties en transportroutes. (Op [www.risicokaart.nl](http://www.risicokaart.nl) kunt u uw mogelijke risicocontour van uw bedrijf raadplegen) |
| Overheidsgebouw | Hiermee wordt het volgende bedoeld: publieke gebouwen welke onder beheer van de landelijke of plaatselijke overheid zijn. Denk hierbij aan: Ministeries, Gemeentelijke kantoren, bibliotheken, politiebureau etc.  |
| Tunnel(ongeval) | Ongevallen in tunnels hebben een hoger effect dan in de buitenlucht, vooral als er brand ontstaat. De hitte kan extreem worden en rook blijft hangen. Mensen kunnen moeilijk vluchten en staan daarom bloot aan de hitte en de rook.  |
| Een risicovolle vervoersbeweging | Enkele bijzonder drukke en mistgevoelige autowegen. Over deze autowegen kan ook vervoer van gevaarlijke stoffen plaatsvinden. Als dat minstens tweemaal per week gebeurt en het lokaal bestuur een vermelding noodzakelijk acht, staat dat op provinciale en gemeentelijke risicokaarten. |
| Kwetsbaar object | Kwetsbare objecten zijn gebouwen waarin zich veel mensen kunnen bevinden en/of gebouwen waar niet-zelfredzame mensen aanwezig zijn (zieken, bejaarden, kinderen). Bijvoorbeeld: kinderdagverblijven, basisscholen, ziekenhuizen, hotels met meer dan 10 bedden of gebouwen met meer dan 25 verdiepingen.  |
| Externe veiligheid | Externe veiligheid is een begrip uit het *Besluit Externe Veiligheid Inrichtingen* *(Bevi)* en beschrijft de kans dat personen in de omgeving van een activiteit waar met gevaarlijke stoffen wordt gewerkt, slachtoffer worden van een ongeval met die stoffen. Beleid rond externe veiligheid moet voorkomen dat als gevolg van ongelukken met gevaarlijks stoffen, slachtoffers buiten de bedrijven of langs transportroutes vallen. Bij gevaar buiten het bedrijf of buiten de (spoor/water/weg), zijn aanvullende veiligheidsregels van kracht. De regels kunnen gelden voor het bedrijf of het vervoer zelf, maar kunnen ook van invloed zijn op de omgeving. Zo is bijvoorbeeld een minimale afstand tussen gevaarbronnen en bebouwing in de omgeving is vastgelegd |
| BRZO-bedrijf | In het Besluit Risico’s Zware Ongevallen (BRZO 1999) staan criteria die aangeven welke inrichtingen (bedrijven) een risico vormen voor de omgeving door de kans op zware ongevallen. Dit hangt samen met de aanwezigheid van gevaarlijke stoffen. Bedrijven die onder dit besluit vallen, heten BRZO-bedrijven. Voor deze bedrijven gelden strengere regels dan voor andere bedrijven. |
| Defensie-inrichtingen | Defensie-inrichtingen zijn kazernes, munitieopslagplaatsen, militaire vliegvelden en schiet- en oefenterreinen. In het Register Risicosituaties Gevaarlijke Stoffen worden alleen de Defensie-inrichtingen geregistreerd waar buiten het terrein beperkingen gelden aan het ruimtegebruik.  |
| Belemmerende factor (hoofd)vaarweg | Objecten welke bij schade een belemmering voor de (hoofd)vaarweg betekenen. Bijvoorbeeld een sluis(deur) en een kraan.  |
| (goederen)spoor | Hieronder valt ook rangeerterrein, de plek die wordt gebruikt voor het samenstellen of splitsen van treinen. |
| Luchthaven (heliport) | Een plaats waar vliegtuigen en/of helicopters kunnen landen en opstijgen.  |
| Gevaarlijke stoffen | Gevaarlijke stoffen zijn stoffen waarvan gebruik, transport of opslag risico’s met zich meebrengen zoals explosiegevaar, brand, giftigheid of radioactiviteit. Voorbeelden van gevaarlijke stoffen zijn LPG, benzine, grondstoffen voor medicijnen, chloor en ammoniak. |
| Buisleidingen | Transport van gevaarlijke stoffen kan plaatsvinden door buisleidingen (pijpleidingen). Deze staan op de risicokaart. Voorbeelden zijn: hoge- en middendrukaardgasleidingen (regionale, nationale en internationale aardgasleidingen) en leidingen voor transport van chemische – soms ook giftige – vloeistoffen of gassen. Meestal zijn het ondergrondse leidingen, maar bovengrondse komen ook voor. |
| Wachtplaats / Wachtsteiger | Een ligplaats in een haven waar schepen tijdelijk ligplaats kunnen nemen om te wachten tot de uiteindelijke ligplaats voor ladingbehandeling vrij is. Of een steiger nabij een sluis waar schepen, die op de volgende schutting wachten ligplaats mogen nemen.  |
| ISPS-plichtige schepen | Dat zijn:* Passagiersschepen met inbegrip van hogesnelheidspassagiersvaartuigen;
* Vrachtschepen met inbegrip van hogesnelheidsvaartuigen met een bruto tonnage van 500 ton of meer;
* Booreenheden welke (mede) gebruikt worden voor de internationale vaart.
 |
| Verblijfsduur | De tijd die tussen het aan- en afmeren van een ISPS-plichtig schip zit. |
| Risicolanden | Landen met havens of havenfaciliteiten waarvan is vastgesteld dat zij geen of onvoldoende effectieve ISPS maatregelen ter beheersing van risico’s hebben genomen. In dit aanvraagformulier wordt de lijst van de *United States Coast Guard (USCG)* gehanteerd*.* Deze USCG lijst wordt regelmatig herzien. |

# **H5 Questionnaire bij aanvraag tot certificering van een havenfaciliteit**

1. **Geografische locatie van de havenfaciliteit[[2]](#footnote-2)**

Geef aan wat voor de locatie van uw havenfaciliteit van toepassing is:
(U kunt meerdere antwoorden selecteren)

[ ]  De faciliteit ligt binnen 500 meter van een tunnel;

[ ]  De faciliteit ligt binnen 500 meter van een (goederen)spoor;

[ ]  De faciliteit ligt binnen 500 meter van een treinstation;

[ ]  De faciliteit ligt binnen 500 meter van een tram/bus halte;

[ ]  De faciliteit ligt binnen 500 meter van een passagiers/ferry terminal;

[ ]  De faciliteit ligt binnen de risicocontour 10-⁶ (plaatsgebonden risicocontour) van een ander bedrijf;

[ ]  De faciliteit ligt binnen 500 meter van een overheidsgebouw;

[ ]  De faciliteit ligt binnen 500 meter van object met een risicovolle vervoersbeweging. Bijvoorbeeld een snelweg of een kruispunt;

[ ]  De faciliteit ligt binnen 500 meter van een kwetsbaar object. Bijvoorbeeld een onderwijsinstelling, een tehuis, of een ziekenhuis;

[ ]  De faciliteit ligt binnen 500 meter van een buisleiding voor gevaarlijke stoffen;

[ ]  De faciliteit ligt binnen 100 meter van een object dat mogelijk een belemmerende factor voor de (hoofd)vaarweg kan betekenen;

[ ]  De faciliteit ligt binnen 500 meter van een bedrijf dat valt onder het Besluit Risico's Zware Ongevallen;

[ ]  De faciliteit ligt binnen 1000 meter van een luchthaven. Bijvoorbeeld een vliegveld of een heliport;

[ ]  De faciliteit ligt binnen 500 meter van een energiecentrale. Bijvoorbeeld een elektriciteitscentrale of een kerncentrale;

[ ]  De faciliteit ligt binnen 500 meter van Defensie-inrichting(en);

[ ]  De faciliteit ligt nabij een ander, hierboven niet genoemd, risicovol aspect, namelijk

Beschrijf hier andere risicovolle aspecten t.a.v. uw faciliteit.

Toelichting:

De omgevingsaspecten van een havenfaciliteit zijn van invloed op de blootstelling van een faciliteit als het effect van een ongewenst incident op de betreffende faciliteit. Geef aan welke omgevingsaspecten voor uw faciliteit van toepassing zijn.

1. **Type ladingbehandeling op de havenfaciliteit**

Selecteer welke ladingbehandeling op uw havenfaciliteit plaatsvindt:
(U kunt meerdere antwoorden selecteren)

[ ]  Passagiers / ferry

[ ]  Containers

[ ]  Ro-Ro

[ ]  Natte bulk /food

[ ]  Natte bulk / non-food

[ ]  Droge bulk / food

[ ]  Droge bulk / non-food

[ ]  General cargo / food

[ ]  General cargo / non-food

[ ]  Offshore base

[ ]  Scheepswerf

[ ]  Wachtplaats

Toelichting:

Het standaard risico profiel van een havenfaciliteit wordt bepaald door het type ladingbehandeling, of de combinatie van ladingbehandeling, op de betreffende faciliteit. Dit wordt op een generieke wijze gevraagd en er zal dus geen verder onderscheid gemaakt worden in soort product/grondstof.

1. **Type ladingsstroom betreffende de havenfaciliteit**

Bestaan er op uw havenfaciliteit ladingstromen van en naar zogenaamde risicolanden?

[ ]  Ja

[ ]  Nee

*Zie bijlage 1 voor de landenlijst*

Toelichting:

Het is van belang om een beeld te hebben van de route die binnenkomende en uitgaande schepen/ladingen afleggen. Ladingstromen van en naar landen met een verhoogd dreigingsbeeld verhogen de blootstelling van een havenfaciliteit en daarmee het risico op een ongewenst incident. Een ‘risicoland’ is misschien een subjectief begrip maar aan de hand van de lijst kunt u beoordelen of uw havenfaciliteit te maken heeft met ladingstromen van of naar dergelijke landen. Deze lijst wordt gefaciliteerd door USCG. Deze organisatie is een expert op dit vakgebied. De lijst is echter dynamisch en onder verandering onderhevig. Geef aan of uw bedrijf ladingstromen heeft van of naar de landen die op de lijst staan.

1. **BRZO**

Valt uw havenfaciliteit als bedrijf onder het Besluit Risico's Zware Ongevallen (BRZO)?

[ ]  Ja

[ ]  Nee

Toelichting:

Het Besluit Risico's Zware Ongevallen (BRZO) integreert wet- en regelgeving op het gebied van arbeidsveiligheid, externe veiligheid en rampbestrijding in één juridisch kader. Doelstelling is het voorkomen en beheersen van zware ongevallen waarbij gevaarlijke stoffen betrokken zijn. Het BRZO stelt hierdoor eisen aan de bedrijven die de drempelwaarde overschrijden. Geef aan of uw bedrijf onder dit besluit valt.

1. **Frequentie ontvangst van ISPS-plichtige schepen.**

Met welke frequentie ontvangt uw havenfaciliteit de komende jaren ISPS-plichtige schepen?

(U kunt maar één antwoord selecteren)

[ ]  Eén schip per kwartaal

[ ]  Eén schip in de maand

[ ]  Eén à twee schepen in de week

[ ]  Drie schepen per week

[ ]  Meer dan drie schepen per week

Toelichting:

De hoogte van de blootstelling van een havenfaciliteit heeft een relatie met het aantal schepen dat ontvangen wordt en de totale verblijfsduur van deze schepen; een hogere frequentie en een langere verblijfsduur is risico verhogend. Maar ook een (zeer) lage frequentie kan het risico verhogen omdat dan de mogelijkheid bestaat dat het bewustzijn omtrent de beveiligingsprocedures kan afnemen. Selecteer welke frequentie voor uw havenfaciliteit, naar verwachting, de komende jaren van toepassing is.

1. **Gemiddelde verblijfsduur schip.**

Wat is de gemiddelde verblijfsduur van een schip op uw havenfaciliteit?

(U kunt maar één antwoord selecteren)

[ ]  1 tot 10 uur

[ ]  10 tot 24 uur

[ ]  1 tot 3 dagen

[ ]  3 tot 7 dagen

[ ]  Langer dan één week

Toelichting:

De hoogte van de blootstelling van een havenfaciliteit heeft een relatie met het aantal schepen dat ontvangen wordt en de totale verblijfsduur van deze schepen; een hogere frequentie en een langere verblijfsduur is risico verhogend.

1. **Permanent of Niet-Permanent beveiligd**

Is uw havenfaciliteitpermanent beveiligd?

[ ]  Ja

[ ]  Nee

Toelichting:

Uw havenfaciliteit is permanent beveiligd indien de maatregelen en procedures, zoals beschreven in het beveiligingsplan continue van kracht zijn; d.w.z. 24 uur per dag, 7 dagen per week. De continuïteit van deze werkwijzen heeft mogelijk een positief effect op het veiligheidsbewustzijn van de medewerkers binnen uw organisatie.

Uw Havenfaciliteit is niet permanent beveiligd indien de maatregelen en procedures, zoals beschreven in het beveiligingsplan alleen van kracht zijn in de periode rondom en tijdens de ontvangst van een ISPS -plichtig schip. In een dergelijk geval wordt de faciliteit voor de ontvangst van het ISPS-plichtige schip ‘secure’ gemaakt door o.a. zgn. *sweep* procedures te volgen. Het gebrek aan continuïteit in de beveiligingswerkzaamheden heeft mogelijk een nadelig effect op het veiligheidsbewustzijn van de werknemers binnen uw organisatie.

# **H6. Deel 2: veiligheidsbewustzijn (security awareness)**

Security awareness betekent zeer letterlijk vertaald “beveiligingsbewustzijn”. Beveiliging (security) is een onderdeel van veiligheid. Wanneer mensen doelbewust een onveilige situatie creëren is er sprake van een beveiligingsincident. Bewustzijn (awareness) heeft te maken met kennis over een bepaald onderwerp, de houding richting een bepaald onderwerp en uiteindelijk met het gedrag wat hier uit voortkomt.

Security awareness = Kennis over beveiliging + houding tegenover beveiliging

 🡪 Gedrag richting beveiliging.

Werknemers zijn veiligheid bewust wanneer zij:

* weten waarom er beveiliging is;
* hoe deze beveiliging er uit ziet voor hun bedrijf;
* betrokken zijn bij de beveiliging in het bedrijf;
* weten hoe beveiligingsincidenten te herkennen;
* weten hoe te handelen met betrekkingen tot beveiliging en incidenten.

Voordelen van veiligheid bewust personeel zijn:

* positieve gevolgen bedrijf continuïteit;
* meer melding en reactie op incidenten;
* sneller en directer herkennen en handelen;
* integrale oplossing voor beveiligingsproblemen;
* werknemers kennen het bedrijf;
* werknemers kennen elkaar;
* snellere opvolging van procedures;
* werknemers creëren niet meer zelf onveilige situaties.

De algehele beveiliging zal zichtbaar verbeteren. Dit levert natuurlijk voordelen op, het vertrouwen van de klant zal toenemen, de efficiëntie binnen het bedrijf zal toenemen, kosten veroorzaakt door beveiligingsincidenten zullen dalen, de verzekeringskosten nemen af en ga zo maar door.

Voor extra naslagwerk wat betreft Security Awareness zie*:* *Handreiking creëren security Awareness, van Gemeentelijk havenbedrijf Antwerpen 2012. Via:* [*http://www.portofantwerp.com/nl/handboek-security-awareness*](http://www.portofantwerp.com/nl/handboek-security-awareness)

1. **Veiligheidsincidenten**

Bent u zich bewust van ISPS gerelateerde incidenten, of bijna incidenten, die zich in de laatste 2 jaar op uw havenfaciliteit hebben plaatsgevonden?

[ ]  Ja

[ ]  Nee

Zo ja, wat was de impact? Beschrijf hier de impact.

En wat zijn maatregelen die uit het incident zijn voortgekomen?

Beschrijf hier de maatregelen.

Toelichting

Het leren van incidenten is een belangrijk onderdeel van veiligheid en het daarbij horende veiligheidsbewustzijn. Wanneer een organisatie leert van incidenten en de geleerde essen gebruikt om haar beveiligingsorganisatie- en andere bedrijfsprocessen te verbeteren, dan kunnen eventuele toekomstige incidenten worden voorkomen. Vandaar dat het zeer belangrijk is dat incidenten en bijna-incidenten gerapporteerd en geanalyseerd worden. De incident historie van uw organisatie en bedrijfsprocessen, en de trend daarin, zegt dus veel over het veiligheidsbewustzijn binnen uw organisatie.

1. **Risico’s met betrekking tot de bedrijfsprocessen.**

Is het personeel op uw havenfaciliteit zich bewust van de mogelijke beveiligingsrisico’s die verbonden zijn aan de bedrijfsprocessen?

[ ]  Ja

[ ]  Nee

Welk rapportcijfer geeft u hiervoor: [ ]  1 - [ ]  2 - [ ]  3 - [ ]  4 - [ ]  5 - [ ]  6 - [ ]  7 - [ ]  8 - [ ]  9 - [ ]  10

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef een toelichting op uw keuze. |

Toelichting

Door veiligheidsbewuste medewerkers wordt de veiligheid in uw organisatie aanmerkelijk vergroot. Risico’s worden eerder (h)erkend, opgelost en gemeld. Daarnaast bevordert veiligheidsbewustzijn het uiteindelijke gewenste veilige gedrag in het werk en beheersing van de gevaren. Door het geven of volgen van bijvoorbeeld een bewustzijnstraining wordt een mentaliteits- en gedragsverandering beoogd op de Havenfaciliteit. De medewerkers zullen een proactieve houding ontwikkelen ten aanzien van veiligheid en hun communicatie bijstellen.

1. **Verschillende vormen van dreiging**

Hoe hoog schat u de risico’s voor de continuïteit van de bedrijfsprocessen en vitale infrastructuur van uw havenfaciliteit met betrekking tot **terrorisme**?

(U kunt maar één antwoord selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef hier een toelichting op uw keuze. |

Toelichting

Definitie: ‘Terrorisme’ is het dreigen met, voorbereiden of plegen van geweld dat gericht is op mensen of op het aanrichten van maatschappij-ontwrichtende schade. Doel hiervan is maatschappelijke veranderingen te bewerkstelligen, de bevolking bang te maken of politieke besluitvorming te beïnvloeden.

Terrorisme is een potentiële dreiging voor de maritieme industrie, omdat schepen en havenfaciliteiten kunnen gebruikt worden om:

* Explosieven te verbergen in de lading
* Terroristen en wapens te smokkelen naar een doelwit in de haven
* Terroristen en wapens Europa in te smokkelen
* Economische en milieu schade te berokkenen, aan de haven of elders
* Gijzelaars te nemen of om de haven zelf te gijzelen
* Als afleiding te dienen voor een aanslag op een andere locatie
* Diefstal van gevaarlijke goederen om aanslagen mee te plegen
* De gevaarlijke goederen die al aanwezig zijn in de haven te gebruiken voor een aanslag in de haven.
1. **Verschillende vormen van dreiging**

Hoe hoog schat u de risico’s voor de continuïteit van de bedrijfsprocessen en vitale infrastructuur van uw havenfaciliteit met betrekking tot **activisme**?

(U kunt maar antwoord item selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):** Geef hier een toelichting op uw keuze. |

Toelichting

Definitie: ‘Activisme’ is de algemene benaming voor het fenomeen waarbij personen of groepen op buitenparlementaire wijze, maar binnen de grenzen van de wet, streven naar verbetering van bepaalde situaties. Denk aan het organiseren van demonstraties en bijeenkomsten. In de praktijk heeft activisme ook uitspattingen naar het extremisme en kunnen ook illegale handelingen plaats vinden.

1. **Verschillende vormen van dreiging**

Hoe hoog schat u de risico’s voor de continuïteit van de bedrijfsprocessen en vitale infrastructuur van uw havenfaciliteit met betrekking tot **criminaliteit**?

(U kunt maar één antwoord selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef hier een toelichting op uw keuze. |

Toelichting

Definitie: ‘Criminaliteit’ is een verzamelbegrip voor alle gedragingen, acties, handelingen en/of gebeurtenissen die volgens de wet strafbaar zijn.

Het globale karakter van de maritieme industrie en de daarin grote hoeveelheid goederen die verhandeld wordt, trekt criminele activiteiten aan. Smokkel staat hierbij bovenaan, immers zelfs bij beveiligde faciliteiten kunnen niet alle goederen geheel worden gecontroleerd.

1. **Omliggende havenfaciliteiten.**

Hoe hoog schat u de risico’s voor de continuïteit van de bedrijfsprocessen en vitale infrastructuur van uw havenfaciliteit met betrekking tot een ongewenste gebeurtenis bij een bedrijf in de directe nabijheid.

(U kunt maar één antwoord selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef hier een toelichting op uw keuze. |

Toelichting

Omgevingsaspecten zijn in de haven puur afhankelijk van de ligging van uw havenfaciliteit en het type terminals dat zich om u heen gevestigd hebben. Analyseer het gebied rondom uw havenfaciliteit met in uw achterhoofd de volgende vraag:

*“Indien een X incident zich afspeelt bij bedrijf Y, wat zijn de gevolgen van dat incident voor het welzijn van de werknemers, de bedrijfsprocessen en de vitale infrastructuur van mijn havenfaciliteit.”*

1. **Cyber Security - continuïteit**

Hoe hoog schat u de risico's voor de continuïteit van de bedrijfsprocessen en vitale infrastructuur van uw havenfaciliteit door een digitale inbreuk op de beveiliging van de computer-, netwerk- en database systemen van uw havenfaciliteit?
(U kunt maar één antwoord selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef hier een toelichting op uw keuze. |

Toelichting

Definitie: Cybersecurity is beveiliging ten behoeve van weerbaarheid (tegen cybercriminaliteit, cyberterrorisme en hacktivisme) in het digitale domein.

Computersystemen verbonden aan internet zijn niet meer weg te denken uit het Nederlandse bedrijfsleven. Met toename van de digitale afhankelijkheden, neemt ook de kans op inbreuk op de digitale beveiliging toe.

Cybercrime tegen het bedrijfsleven richt zich meestal op het verkrijgen van toegang tot kapitaal. Ook kunnen cybercriminelen er op uit zijn om bedrijfs- en productieprocessen te verstoren.

1. **Cyber Security - beveiliging**

Hoe hoog schat u de impact op de totale beveiliging van uw havenfaciliteit door een digitale inbreuk op de beveiliging van de computer-, netwerk- en database systemen van uw havenfaciliteit?
(U kunt maar één antwoord selecteren)

[ ]  Hoog

[ ]  Midden

[ ]  Laag

|  |
| --- |
| **Toelichting keuze (PFSO):**Geef hier een toelichting op uw keuze. |

Toelichting

Definitie: Cybersecurity is beveiliging ten behoeve van weerbaarheid (tegen cybercriminaliteit, cyberterrorisme en hacktivisme) in het digitale domein.

Computersystemen verbonden aan internet zijn niet meer weg te denken uit het Nederlandse bedrijfsleven. Hoe hoog schat u het risico ten aanzien van onder meer:

* Digitale benadering van uw beveiligingsplan en procedures;
* Manipulatie van digitale beveiligingssystemen zoals camera’s;
* Via digitale manipulatie toegang verschaffen tot de faciliteit.

# **H7. Ondertekening door PFSO**

|  |
| --- |
| Naar waarheid ingevuld door:Naam : Type hier uw volledige naam.Functie : Type hier uw volledige functie.Datum : Type hier de datum.Handtekening : |

# **Bijlagen**

**Risicolanden**

Landen met havens of havenfaciliteiten waarvan is vastgesteld dat zij geen of onvoldoende effectieve ISPS maatregelen ter beheersing van risico’s hebben genomen. In dit aanvraagformulier wordt de lijst van de *United States Coast Guard (USCG)* gehanteerd*.* Deze USCG lijst wordt regelmatig herzien.

De lijst hieronder geeft de landen weer die niet aan de eisen voldoen:

* Cambodja
* Kameroen
* Comoren
* Ivoorkust
* Cuba
* Equatoriaal Guinea
* Gambia
* Guinea-Bissau
* Iran
* Liberia
* Libië
* Madagaskar
* Nigeria
* Sao Tome and Principe
* Syrië
* Oost-Timor
* Venezuela
* Yemen

Schepen die op weg naar Nederland zijn en één van de bovenstaande landen in hun laatste vijf haven heeft aangedaan moeten de volgende stappen nemen:

1. Uitvoering van de maatregelen verkondigd in het veiligheidsplan voor veiligheidsniveau 2;
2. Zorgen ervoor dat elk toegangspunt tot het schip wordt bewaakt, de bewakers hebben daarnaast een totaal overzicht van de buitenkant van het schip;
3. poging om een ​​verklaring van de beveiliging uit te roepen;
4. alle veiligheid acties in het logboek van de schip beveiliging administratie te voeren;
5. rapport maatregelen genomen om het bewust US Coast Guard kapitein van de ( geplande aankomst ) poort voor aankomst in de haven.

Voor de uitzonderingen van havens binnen een land raadpleeg de site:

<http://www.uscg.mil/>

<https://homeport.uscg.mil/mycg/portal/ep/contentView.do?channelId=-18389&contentId=522201&programId=63715&programPage=%2Fep%2Fprogram%2Feditorial.jsp&pageTypeId=13489&contentType=EDITORIAL&BV_SessionID=@@@@1895900799.1452604846@@@@&BV_EngineID=ccccadgifigjkfjcfngcfkmdfhfdfgn.0>

1. De Internationale Code voor de Beveiliging van Schepen en Havenfaciliteiten (International Ship and Port facility Security Code) is van toepassing op passagiersschepen en overige schepen > 500 GT welke internationale zeereizen maken. [↑](#footnote-ref-1)
2. Via [www.risicokaart.nl](http://www.risicokaart.nl) kunt u eenvoudig de risico's bij u in de buurt traceren door uw postcode in te voeren. [↑](#footnote-ref-2)